Revogada pela Resolução nº 340/2023

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

RESOLUÇÃO Nº 298, DE 4 DE AGOSTO DE 2021

Dispõe sobre a Política de Privacidade, Segurança Cibernética e Gestão de Dados Abertos na Justiça Militar da União.

O SUPERIOR TRIBUNAL MILITAR, no uso das atribuições que lhe são conferidas pelo Regimento Interno do Superior Tribunal Militar, e

CONSIDERANDO que a segurança da informação é multidisciplinar e não deve estar limitada à tecnologia da informação;

CONSIDERANDO as recomendações relativas à governança de Tecnologia da Informação - TI, à segurança da informação e a preservação da informação do Tribunal de Contas da União e do Conselho Nacional de Justiça;

CONSIDERANDO que é imprescindível garantir a segurança cibernética da Justiça Militar da União;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de segurança da informação, alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;

CONSIDERANDO o que dispõe a Lei nº 13.709, de 14 de agosto de 2018, com a redação dada pela Lei nº 13.853, de 8 de julho de 2019, sobre a proteção de dados pessoais;

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

CONSIDERANDO a Resolução nº 240, de 19 de abril de 2017, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, na Justiça Militar da União e dá outras providências;

CONSIDERANDO a Resolução nº 222, de 3 de fevereiro de 2016, que institui a Política de Segurança da Informação e Comunicação da Justiça Militar da União e dá outras providências;

CONSIDERANDO a Resolução nº 265, de 6 de junho de 2019, que institui a Política de Gestão Documental da Justiça Militar da União (JMU);

CONSIDERANDO a necessidade de estabelecer diretrizes para a gestão de identidades e credenciais visando ao controle de acesso aos sistemas, equipamento de tecnologia da informação e serviços;

CONSIDERANDO a importância de instituir uma política interna de dados abertos;

CONSIDERANDO a necessidade de se estabelecer ações em caso de riscos e incidentes quanto à segurança cibernética;

CONSIDERANDO que, para contemplar aspectos fundamentais para o desenvolvimento da política sobre a área da segurança cibernética, será necessário abordar aspectos da Segurança da Informação, área sistêmica e mais abrangente;

CONSIDERANDO a deliberação do Plenário na 11ª Sessão Administrativa, realizada em 4 de agosto de 2021, ao apreciar o Expediente Administrativo nº 22/2021;

R E S O L V E:

Art. 1º Instituir a Política de Privacidade, Segurança Cibernética e Gestão de Dados Abertos na Justiça Militar da União, na forma do Anexo I.

Parágrafo único. A Política de Privacidade, Segurança Cibernética e Gestão de Dados Abertos tem por objetivos preventivos a proteção e a preservação dos dados, da infraestrutura tecnológica, dos processos e documentos produzidos, recebido e custodiados, no âmbito da Justiça Militar da União (JMU), de modo a prevenir e mitigar a ocorrência de vulnerabilidades, sendo aplicável em qualquer meio ou suporte.

Art. 2º Todos os procedimentos referentes à Privacidade, Segurança Cibernética e Gestão de Dados Abertos deverão ser publicados em veículo interno da Justiça Militar.

Art. 3º Ficam revogados:

I - a Resolução nº 194, de 28 de agosto de 2013;

II - a Resolução nº 222 de 3 de fevereiro de 2016;

III- a Resolução nº 226 de 24 de agosto de 2016; e

IV - o Ato Normativo nº 137, de 12 de maio de 2015.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

Gen Ex **LUIS CARLOS GOMES MATTOS**
Ministro-Presidente

POLÍTICA DE PRIVACIDADE, SEGURANÇA CIBERNÉTICA E GESTÃO DE DADOS ABERTOS NA JUSTIÇA MILITAR DA UNIÃO

ANEXO I

APRESENTAÇÃO

Esta política tem caráter estratégico e deve ser atendida por todos os níveis hierárquicos, visando à eficácia na proteção das informações e destina-se a estabelecer as diretrizes e os princípios da segurança cibernética, da privacidade e dos dados abertos. Tem por objetivo nortear a implementação de medidas de proteção, que deverão ser aplicadas às informações que têm valor, independentemente de seu suporte material ou tecnológico - ativo de informação.

CAPÍTULO I

Seção I

Das Disposições Preliminares

Art. 1º Para os efeitos desta Resolução consideram-se:

I - acessibilidade: garantia de que pessoa física ou determinado sistema, órgão ou entidade autorizados obtenham acesso à informação e aos arquivos correspondentes sempre que necessitarem, respeitando-se a legislação em vigor;

II - ativo crítico de informação: toda e qualquer informação ou sistema de dados, que tenha valor fundamental para a gestão de processos ou de pessoas, cujo acesso ou destruição possam causar danos ou prejuízos à Justiça Militar da União;

III - autenticidade: qualidade da informação que foi produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema e que está livre de adulteração ou qualquer outro tipo de corrupção;

IV - cadeia de custódia: ininterrupta manutenção da custódia de dados e documentos - desde o seu produtor até o seu legítimo sucessor - pela qual se assegura que são os mesmos desde suas gêneses, não sofreram nenhum processo de adulteração indevido e, portanto, são autênticos, por meio de registros de controles, transferências, análises e disposição de evidências físicas ou eletrônicas, atestados em metadados padronizados, que asseguram o histórico de alterações e guarda dos dados e documentos;

V - ciclo de vida dos dados: todas as etapas de manuseio dos dados, desde o surgimento na instituição até sua destinação final - o respectivo descarte ou guarda e manutenção permanentes;

VI - confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizados e credenciados;

VII - controlador: pessoa jurídica de direito público a quem compete definir todas as ações relativas ao tratamento dos dados pessoais;

VIII - custodiante dos ativos de informação: qualquer indivíduo, órgão ou unidade administrativa que tenha a responsabilidade formal de proteger um ou mais ativos de informação, sendo o responsável por aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, determinadas pelo proprietário dos ativos de informação;

IX - dados abertos: conjunto de dados governamentais produzidos, coletados ou custodiados por autoridades públicas e disponibilizados em formato aberto, que podem ser utilizados, reutilizados e redistribuídos por qualquer pessoa sem restrições de direito de autor, patente ou outro mecanismo de controle e que estejam sujeitos às exigências de citação das fontes;

X - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XI - documento: unidade de registro de informação, em qualquer suporte ou formato;

XII - encarregado pelo tratamento dos dados pessoais: pessoa física ou jurídica responsável por, dentre outras atribuições, realizar a comunicação entre a Autoridade Nacional de Proteção de Dados e o Controlador, bem como conhecer detalhadamente todo o tratamento efetivado de dados pessoais na instituição;

XIII - *file server*: computador conectado a uma rede que fornece um local para acesso ao disco compartilhado, armazenamento de arquivos de computador, como texto, imagem, som, vídeo, que podem ser acessados pelas estações de trabalho que são capazes de alcançar o computador que compartilha o acesso por meio de uma rede de computadores;

XIV - informação: dados utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XV - integridade: qualidade da informação não modificada ou destruída, inclusive quanto à origem, trânsito e destino;

XVI - *malware*: código ou programa maliciosos, *software* nocivo, *software* mal-intencionado destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos e alterações;

XVII - operador: pessoa física que realiza o tratamento em nome do controlador, em todas as instâncias da instituição ou no âmbito de contratos ou instrumentos congêneres firmados com ele;

XVIII - segurança cibernética: segurança física e proteção de dados pessoais, institucionais, além de ativos de tecnologia da informação de forma geral;

XIX - segurança da informação: conjunto de medidas e ações necessárias por garantir que a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações de uma organização ou indivíduo foram preservadas;

XX - sistema de negócios: conjunto de tecnologias que se relacionam, coletando, armazenando, processando e apresentando informações a determinados usuários, que as acessam por meio de um mecanismo de autenticação em um sistema informatizado, como objetivo maior de apoiar e/ou viabilizar a execução de processos de negócios, bem como a tomada de decisões em uma organização;

XXI - tratamento da informação: conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, avaliação, destinação, eliminação ou controle da informação;

XXII - *trojan*: programa que acessa o computador ou aplicativo disfarçado de programa comum e legítimo que permite que seu computador seja controlado remotamente e/ou seja utilizado como meio para invasões ao ambiente interno de uma Organização;

XXIII - transparência ativa: princípio que exige de órgãos e entidades públicas a divulgação de informações de interesse geral, independentemente de terem sido solicitadas;

XXIV - usuário de Tecnologia da Informação e Comunicação - TIC: qualquer usuário que utiliza recursos de Tecnologia da Informação da Justiça Militar da União.

Seção II

Das Finalidades

Art. 2º A segurança cibernética abrange aspectos físicos, tecnológicos e humanos e orienta-se pelos princípios de autenticidade, confidencialidade, disponibilidade e integridade e pelas seguintes regras:

I - ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade da prestação jurisdicional e administrativa dos órgãos do Poder Judiciário;

II - ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética;

III - ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética;

IV - ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de profissionais que atuam de forma direta ou indireta na área de segurança cibernética e da informação;

V - contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio de ações de segurança cibernética, observados os direitos e as garantias fundamentais;

VI - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética;

VII - fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;

VIII - fortalecer a cultura de segurança cibernética no âmbito da Justiça Militar da União;

IX - aprimorar o nível de maturidade em segurança cibernética na Justiça Militar da União;

X - orientar ações relacionadas:

a) à gestão em segurança da informação;

b) à segurança da informação das infraestruturas críticas;

c) ao tratamento das informações com restrições de acesso;

d) à proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com legislação específica;

e) à prevenção, ao tratamento e à resposta a incidentes cibernéticos;

f) à gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos;

g) ao estabelecimento dos níveis de maturidade em segurança cibernética; e

h) ao estabelecimento de processo transparente de comunicação e respostas a incidentes entre o poder público e a sociedade.

Seção III

Das Diretrizes

Art. 3º As diretrizes básicas da Política de Privacidade, Segurança Cibernética e Gestão de Dados Abertos devem ser divulgadas em todas as unidades administrativas da JMU, garantindo que todos tenham consciência da Política e a pratiquem.

Art. 4º Programas continuados de conscientização sobre a segurança cibernética serão implementados assegurando que todos os usuários sejam informados sobre a exigência de garantir acesso à informação como regra geral e sobre os potenciais riscos de segurança e o tipo de tratamento a que estão submetidas as informações de caráter sigiloso ou restrito.

Art. 5º Os processos e os procedimentos para garantir à privacidade seguem as seguintes diretrizes:

I - levantamento e mapeamento dos fluxos dos dados pessoais tratados na Justiça Militar da União;

II - verificação da conformidade do tratamento com o previsto na Lei Geral de Proteção de Dados (LGPD);

III - definição do modo de prestar as informações sobre o tratamento de dados pessoais;

IV - definição do ciclo de vida das informações pessoais e da necessidade de consentimento para utilização de dados pessoais em âmbito administrativo da Justiça Militar da União.

CAPÍTULO II

Seção I

Da Privacidade e Da Proteção Dos Dados Pessoais

Art. 6º O tratamento de dados pessoais, inclusive nos meios digitais, na Justiça Militar da União será realizado pelos seguintes agentes:

I - Controlador e Controlador Adjunto

II - Encarregado

III - Operador

Art. 7º O exercício da função de Controlador e Controlador Adjunto é atribuído, respectivamente, ao Ministro-Presidente e ao Ministro Vice-Presidente no seu ofício de Ministro-Corregedor.

§ 1º Os Controladores serão assessorados pelo Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos, e os servidores e colaboradores que exerçam atividade de tratamento de dados pessoais na instituição ou terceiros, em contratos e instrumentos congêneres firmados com a JMU.

§ 2º O Controlador Adjunto atuará em substituição legal do Controlador.

Art. 8º A função de Encarregado será exercida pelo Ministro-Ouvidor.

Art. 9º O exercício da função de Operador será exercido:

I - pelo Diretor-Geral;

II - pelos diretores no Superior Tribunal Militar e na primeira instância pelos diretores de secretaria;

III - pelos coordenadores;

IV - pelos supervisores e chefes de núcleos.

§ 1º Deverá ser desenvolvida metodologia de controle do tratamento de dados pessoais, que permita a revisão do fluxo dos dados.

Art. 10. Compete ao Controlador e ao Controlador Adjunto:

I - realizar a governança e fornecer as instruções para a política de privacidade dos dados pessoais;

II - determinar a capacitação dos operadores, para que atuem com responsabilidade, critério e ética;

III - ordenar a observância das instruções e das normas sobre a matéria na JMU; e

IV - determinar a permanente atualização desta Política e o desenvolvimento dos respectivos programas.

Art. 11. Compete ao Encarregado:

I - ser o canal de comunicação entre a Justiça Militar da União e:

a) o titular de dados pessoais;

b) a Autoridade Nacional de Proteção de Dados Pessoais.

II - prestar esclarecimentos, realizar comunicações, orientar operadores e contratados sobre as práticas adotadas ou a serem adotadas para garantir a proteção dos dados pessoais;

III - determinar a publicidade da dispensa de consentimento para o tratamento de dados pessoais;

IV - receber as reclamações dos titulares quanto ao tratamento de seus dados, respondê-las e tomar providências para sanar os desvios;

V - deter amplo e sólido conhecimento sobre a legislação de proteção de dados pessoais e normas correlatas;

VI - realizar o atendimento dos titulares de dados pessoais internos e externos à JMU;

VII - manter a comunicação sobre o tratamento de dados pessoais com as autoridades internas e externas;

VIII - apoiar a implementação e a manutenção de práticas de conformidade à legislação sobre o tratamento de dados pessoais;

IX - estabelecer campanhas educativas no órgão sobre o tratamento de dados pessoais;

X - responder a incidentes no tratamento de dados pessoais.

Art. 12. Compete aos Operadores em todos os níveis:

I - documentar as operações que lhe cabem realizar durante o processo de tratamento de dados pessoais;

II - proteger a privacidade dos dados pessoais desde seu ingresso na JMU;

III - descrever os tipos de dados coletados;

IV - utilizar metodologia de coleta dos dados pessoais que considere a minimização necessária para alcançar a finalidade do processo.

Art. 13. O Controlador e os Operadores respondem solidariamente por todo tratamento inadequado dos dados pessoais dos quais resulte, dentre outros, prejuízo ao titular e comprometimento da confiabilidade da JMU.

Art. 14. Os órgãos da Justiça Militar da União poderão realizar o tratamento mínimo dos dados pessoais, necessário e imprescindível à garantia do interesse público e à execução de suas funções jurisdicional e administrativa.

Art. 15. O Superior Tribunal Militar deverá publicar em lugar de fácil acesso e visualização em seu portal na internet:

I - as hipóteses que fundamentam a realização do tratamento de dados pessoais;

II - a previsão legal, a finalidade e os procedimentos para tratamento de dados pessoais;

III - a identificação do Controlador e o contato de correio eletrônico;

IV - o nome do Encarregado e o contato de correio eletrônico;

V - as responsabilidades dos Operadores envolvidos no tratamento e os direitos do titular com menção expressa ao art. 18 da LGPD.

Art. 16. O tratamento dos dados pessoais deverá ser realizado durante todo o ciclo de vida dos documentos.

Seção II

Das Penalidades

Art. 17. O descumprimento das disposições constantes nesta Política e nas normas complementares sobre segurança cibernética e da informação, privacidade e dados abertos caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

CAPÍTULO III

Seção I

Da Estrutura Da Segurança Cibernética e Da Informação

Art. 18. A segurança cibernética e da informação é baseada em três fundamentos:

I - segurança física: baliza a definição das políticas e procedimentos que tratam dos controles de acesso a dados, informações, processos e documentos em quaisquer suportes, nato-digitais ou digitalizados e a equipamentos de informática de propriedade da JMU;

II - segurança dos recursos humanos: visa garantir que quaisquer pessoas que tenham vínculo estatutário, funcional, contratual ou processual com a JMU entendam suas responsabilidades e atuem em consonância com os preceitos da política corporativa de segurança cibernética e da informação, para que o risco de furto, fraude ou mau uso de informações seja limitado ou reduzido;

III - segurança lógica: forma como os ativos de tecnologia são protegido, por *softwares* ou regras de restrições de acesso, como proteção contra ataques, proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação, e de prevenção e proteção contra ataques cibernéticos, vírus e *malware*.

Art. 19. A Política de Privacidade, Segurança Cibernética e Gestão de Dados Abertos é composta pelos seguintes temas:

I - classificação da informação;

II - gestão de riscos de segurança da informação;

III - gestão de incidentes em segurança da informação;

IV - garantia e controle de acesso à informação;

V - segurança da informação em recursos humanos;

VI - gestão de equipamentos de informática;

VII - gestão de ativos e serviços de tecnologia da informação e comunicação;

VIII - gestão de cópias de segurança;

IX - gestão de dispositivos móveis no trabalho remoto;

X - análise crítica da segurança da informação;

XI - proteção de dados pessoais;

XII - capacitação e conscientização em segurança da informação;

XIII - gestão de dados abertos; e

XIV - ação de governança cibernética para elevar o nível de segurança da infraestrutura críticas.

Parágrafo único. Os temas listados no *caput*, e outros que venham a surgir, serão definidos em normativos específicos a serem estruturados e monitorados, de forma a permitir sua melhoria contínua.

Seção II

Do Uso Dos Recursos De Tecnologia Da Informação

Art. 20. Os recursos de tecnologia da informação disponibilizados aos usuários de Tecnologia da Informação e Comunicação (TIC) destinam-se ao atendimento das necessidades do serviço, das necessidades informacionais da JMU e a transparência ativa respeitando a legislação vigente.

§ 1º Para fortalecer as ações de governança cibernética, deve-se estabelecer um sistema de gestão em segurança da informação baseado em riscos.

§ 2º É proibida a utilização dos recursos de tecnologia da informação disponibilizados pela Justiça Militar da União para acesso, guarda e divulgação de material incompatível com o ambiente do serviço, que viole direitos autorais, ou que infrinja a legislação vigente.

§ 3º Fica proibido o armazenamento no *file server* da JMU de arquivos para uso pessoal, os quais não possuem relações com as atividades institucionais que desempenham ou com as competências dos órgãos da JMU, independentemente de formato de criação ou armazenamento, incluindo filmes, vídeos, músicas, apostilas, livros, fotografias, entre outros.

§ 4º É vedada a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela JMU.

Art. 21. Aos usuários de TIC serão fornecidos mecanismos de identificação, autenticação e autorização baseados em *login* e senha e/ou certificação digital, de uso pessoal e intransferível, vedada sua divulgação a terceiros.

Art. 22. Todas as operações realizadas com uso dos recursos de tecnologia da informação poderão ser registradas para fins de auditoria tecnológica.

Seção III

Da Conformidade

Art. 23. Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto ao uso, à disponibilização e à disseminação de informações públicas ou protegidas, tais como dados pessoais relativos à intimidade, à vida privada, à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais e de indústria, patentes e marcas registradas ou aquelas classificadas como sigilosas.

Art. 24. Os sistemas de informações, além de disponibilizar os registros em prazos e formatos que atendam as exigências legais, devem garantir autenticidade, integridade, disponibilidade, originalidade, organicidade, unicidade, fidedignidade, imparcialidade, não repúdio e, quando for o caso, confidencialidade das informações.

Art. 25. Será implementada a gestão de usuários de sistemas informatizados composta de:

I – gerenciamento de identidades;

II – gerenciamento de acessos; e

III – gerenciamento de privilégios.

Parágrafo único. A gestão de usuários será disciplinada por Ato Normativo do Presidente, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo

de uniformizar e garantir a experiência única de interação com os sistemas judiciais.

Seção IV

Dos Ativos De Informação e Da Gestão De Riscos

Art. 26. O plano de gestão de riscos da segurança cibernética alinha-se à política de gestão de riscos da Justiça Militar da União.

§ 1º Cada unidade administrativa e órgão deve identificar todos os seus ativos bem como manter e estruturar um inventário de ativos de informação críticas, tendo em vista a gestão de riscos de segurança cibernética e da informação.

§ 2º O inventário deve documentar e classificar a importância do ativo para o negócio, o impacto para as atividades finalísticas em caso de comprometimento e a estratégia que permita a recuperação do ativo em caso de desastre.

§ 3º Todos os ativos críticos devem ter um proprietário formalmente designado.

§ 4º O proprietário dos ativos de informação é a parte interessada do órgão ou unidade administrativa, ou indivíduo legalmente instituído por sua posição e cargo, o qual é responsável por:

I - assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificadas em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada, segundo a Resolução nº 240, de 19 de abril de 2017;

II - delegar formalmente as tarefas de rotina de gestão da informação a um custodiante.

§ 5º Os riscos da informação devem ser adequadamente gerenciados por atividades de controles internos.

§ 6º As regras para o uso das informações, dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas.

§ 7º Os usuários que têm acesso aos ativos da JMU devem cumprir os requisitos de segurança associados à informação e aos recursos de processamento.

§ 8º A definição e a publicação do programa de gerenciamento de riscos do tratamento de dados pessoais na Justiça Militar da União é responsabilidade do Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA).

§ 9º Para elevar o nível de segurança das infraestruturas críticas, adotar-se-á as seguintes critérios:

I - estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão;

II - instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

III - elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa;

IV - utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança;

V - utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

VI - providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes;

VII - elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares;

VIII - elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto;

IX - adotar práticas e requisitos de segurança cibernética no desenvolvimento de novos projetos, tais como dupla verificação do acesso externo;

X - realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos;

XI - realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; e

XII - estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado com objetivo colaborativo.

SEÇÃO V

Do Plano De Continuidade

Art. 27. Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos e atenderão aos seguintes objetivos:

I - avaliar em regime emergencial, as consequências de desastres, falhas de segurança e perda de serviços;

II - contingenciar e recuperar o funcionamento normal dentro de períodos de tempo determinados;

III - recuperar tempestivamente as operações consideradas vitais.

Art. 28. Compete ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos consolidar, monitorar e revisar periodicamente o plano de continuidade em regulamento específico.

Parágrafo único. As unidades administrativas e órgãos da Justiça Militar da União ficam obrigados a apresentar o plano de continuidade de sua área e um relatório anual de monitoramento.

Seção VI

Gerenciamento De Crises e Incidentes Cibernéticos

Art. 29. Fica criado o Comitê de Crises e Incidentes Cibernéticos, formado pela composição do Comitê de Governança de Tecnologia da Informação e Comunicação e do Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA).

§ 1º As reuniões do Comitê de Crises e Incidentes Cibernéticos ocorrerão em local específico seguro e com recursos estabelecidos para gerir as situações de crise.

Art. 30. A gestão de incidentes em segurança cibernética e da informação tem por objetivo assegurar que fragilidades e incidentes em segurança cibernética sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

§ 1º Detectados eventuais incidentes cibernéticos que coloquem em risco a segurança cibernética, fica a Diretoria de Tecnologia da Informação autorizada a desligar todos os serviços de tecnologia da informação e comunicação.

§ 2º Magistrados, servidores e quaisquer colaboradores da JMU são responsáveis por:

I - informar imediatamente ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos os incidentes com a segurança cibernética a que tenham dado causa, de que tenham ciência ou suspeita;

II - colaborar na respectiva área de competência, com a identificação e o tratamento de incidentes, em segurança da informação.

Art. 31. As violações de segurança devem ser comunicadas e registradas, e esses registros analisados periodicamente, com o propósito de caráter corretivo, legal e de auditoria.

Art. 32. Em caso de incidente cibernético, o Comitê de Governança de Tecnologia da Informação e Comunicação instituirá formalmente o Comitê de Investigação para Ilícitos Cibernéticos, baseados no relatório do Comitê de Crises e Incidentes Cibernéticos.

§ 1º O Comitê de Investigação para Ilícitos Cibernéticos estabelecerá os procedimentos básicos para coleta e preservação de evidências.

§ 2º O Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação comunicará de imediato ao órgão de polícia com atribuição para apurar os fatos.

§ 3º Representantes da área atingida pelo incidente cibernético comporá o Comitê de Investigação para Ilícitos Cibernéticos.

Seção VII

Da Preservação Digital De Documentos

Art. 33. A preservação digital engloba todos os dados e documentos arquivísticos nato-digitais ou digitalizados, administrativos ou judiciais, produzidos ou recebidos pela Justiça Militar da União em decorrência de suas atividades.

Parágrafo único. Os documentos arquivísticos digitais são:

I - processos administrativos ou judiciais digitais;

II - informações arquivísticas produzidas nos sistemas de negócios do Tribunal;

III - gravações digitais de som e imagem;

IV - fotografias digitais;

V - páginas intranet e internet;

VI - bases de dados digitais;

VII - publicações digitais;

VIII - mensagens de correio eletrônico quando se tratar de assunto institucional.

Art. 34. A preservação digital tem como princípios:

I - organização e preservação dos documentos digitais e de todos os seus componentes, de modo a garantir a disponibilidade plena desses registros no futuro;

II - integridade e confiabilidade das informações custodiadas, de modo a garantir a segurança dos documentos e evitar a corrupção e a perda de dados;

III - garantia de autenticidade dos documentos;

IV - respeito à propriedade intelectual;

V - observância do sigilo e da restrição de acesso às informações sensíveis;

VI - transparência ativa;

VII - descrição multinível de documentos digitais avaliados como de guarda permanente;

VIII - avaliação arquivística de acordo com o Plano de Classificação e Tabela de Temporalidade da JMU.

Art. 35. Os objetivos da preservação digital são:

I - implantar repositório arquivístico digital confiável – RDC-Arq, para receber, descrever, armazenar, preservar e garantir o acesso contínuo aos documentos arquivísticos digitais custodiados;

II - tornar público o contexto de implantação da preservação digital, bem como os requisitos legais e os normativos com os quais o Tribunal está em conformidade;

III - fundamentar a definição dos procedimentos e as opções tecnológicas a serem adotadas no tratamento da informação digital;

IV - divulgar as estratégias adotadas com relação à abordagem de preservação digital, de modo a propiciar o seu aperfeiçoamento contínuo;

V - assegurar as condições adequadas ao pleno acesso a documentos digitais, pelo prazo institucionalmente estabelecido e respeitado o Plano de Classificação e Tabela de Temporalidade da JMU;

VI - zelar pela cadeia de custódia de modo permanente, com o intuito de garantir a autenticidade dos documentos digitais;

VII - contribuir para a cultura da gestão de risco em segurança da informação;

VIII - promover o intercâmbio de informações e experiências com entidades públicas e privadas, nacionais e internacionais, com vistas à constante atualização e aperfeiçoamento das normas e procedimentos de preservação digital do Tribunal;

IX - fomentar a capacitação sistemática na área de preservação digital;

X - estabelecer atributos e solução para o armazenamento no *file server;*

XI - permitir o acesso à informação de forma objetiva.

Art. 36. A produção, o recebimento e a captura de documentos digitais no âmbito do Tribunal obedecerão aos seguintes requisitos de preservação digital:

I - classificação arquivística dos documentos em sua origem, de acordo com as normas vigentes referentes à gestão documental;

II - registro do conjunto mínimo de metadados descritivos de preservação dos documentos;

III - observância da padronização de formatos de arquivos para documentos de guarda longa ou permanente;

IV - migração de *hardware*, *software*, formato e metadados com informações técnicas que permitam avaliar a qualidade da migração;

V - observância da cadeia de custódia e da cadeia de preservação digital;

VI - padronização das mídias de gravação e armazenamento;

VII - capacidade de migração automática de formatos, a fim de superar a obsolescência tecnológica e digital, sem intervenção manual, sem rompimento da cadeia de custódia e sem perda de autenticidade.

Art. 37. Os requisitos de preservação digital adotados e os padrões e procedimentos operacionais necessários à sua implantação serão normatizados pelo Plano de Preservação de Documentos Digitais (PPDD) e amplamente divulgados, sendo oferecida aos interessados a devida orientação técnica.

Art. 38. O Repositório Arquivístico Digital Confiável (RDC-Arq) será composto de:

I - *software* de dados abertos que atenda às necessidades de preservação digital de processos e documentos judiciais e administrativos;

II - procedimentos normativos e técnicos capazes de manter íntegros e autênticos os documentos digitais nele custodiados, de modo a preservá-los e acessíveis pelo tempo necessário.

Art. 39. Somente serão encaminhados e aceitos no RDC-Arq os documentos arquivísticos digitais consolidados, em sua versão final, e que tenham sido submetidos a avaliação e seleção documental pela Comissão Permanente de Avaliação e Apoio Técnico à Gestão Documental da Justiça Militar da União (CPAT-JMU).

§ 1º Os documentos digitais de guarda permanente deverão obrigatoriamente ser recolhidos ao RDC-Arq e terão prioridade de recursos em relação aos demais no repositório.

§ 2º Os documentos arquivísticos digitais de guarda longa, ainda que não estejam destinados à guarda permanente, serão transferidos ao repositório e nele mantidos pelos prazos estabelecidos na Tabela de Temporalidade.

§ 3º Os documentos digitais aceitos no RDC-Arq deverão atender aos requisitos de acesso e recuperação integral de seu conteúdo, de forma a serem lidos e compreendidos independentemente dos sistemas que os produziram.

§ 4º Os documentos digitais enviados ao RDC-Arq deverão constar de um pacote de informações que identifique suas características arquivísticas, em especial os metadados descritivos e administrativos.

§ 5º Os documentos digitais permanentes aceitos no RDC-Arq e seus respectivos pacote de informações deverão ter seu histórico de produção e de manutenção e seus respectivos metadados preservados indefinidamente, por meio da cadeia de custódia.

Seção VIII

Do Comitê Executivo De Privacidade, Segurança Cibernética e Dados Abertos

Art. 40. Fica criado o Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA).

§ 1º O Comitê Executivo será subordinado ao Diretor-Geral.

§ 2º O Comitê Executivo será composto por:

I - Diretor(a) de Documentação e Gestão do Conhecimento, como Coordenador(a) Negocial;

II - Diretor(a) de Tecnologia da Informação, como Coordenador(a) Técnico(a);

III - Diretor de Secretaria da Corregedoria;

IV - Coordenador(a) de Tecnologia;

V - Coordenador(a) de Apoio Jurisdicional;

VI - Coordenador(a) do Comitê Executivo do SEI-JMU.

§ 3º O Comitê Executivo será o gestor institucional de segurança da informação.

§ 4º Nas ausências e impedimentos legais do(a) Coordenador(a) Negocial, o(a) Coordenador(a) Técnico(a) do Comitê assumirá as suas atribuições.

§ 5º Os demais membros do Comitê, em suas ausências e impedimentos legais ou regulamentares, conforme as necessidades serão representados pelos seus substitutos automáticos.

§ 6º O Coordenador Negocial do Comitê poderá solicitar servidores de outras áreas e convidados externos para participar das reuniões, em função dos assuntos a serem tratados.

Art. 41. Compete ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos:

I - elaborar e submeter ao Comitê de Governança de Tecnologia da Informação e Comunicação estudos sobre planejamento, controle e ações de segurança cibernética;

II - determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança cibernética e à tomada de decisão;

III - definir as metas estratégicas de segurança cibernética e da informação na Justiça Militar da União;

IV - propor o Plano de Gestão da Continuidade de Negócios que identifique as atividades críticas, avalie os riscos e defina estratégias de continuidade, de forma a evitar ou mitigar as perdas em potencial;

V - formular e conduzir diretrizes para o Sistema de Gestão de Segurança Cibernética e da Informação, considerando as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD);

VI - identificar os agentes de tratamento de dados pessoais referidos na legislação federal, bem como definir suas atribuições e responsabilidades;

VII - elaborar diretrizes para o tratamento adequado dos dados pessoais em cadastros, bases de dados e sistemas da JMU, visando à proteção desses dados;

VIII - elaborar relatório de impacto para proteção de dados pessoais, que deve descrever processos de tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como conter medidas, salvaguardas e mecanismos de mitigação desses riscos;

IX - propor ações de tratamento de dados pessoais;

X - propor a elaboração e a revisão de normas e de procedimentos relativos à segurança cibernética, privacidade e dados abertos;

XI - manifestar-se sobre matérias que lhe sejam submetidas atinentes à segurança cibernética, privacidade e dados abertos;

XII - assessorar o Comitê de Governança de Tecnologia da Informação e Comunicação em matéria correlata à segurança cibernética;

XIII - manter-se alinhado às diretrizes da governança institucional relativas ao subsistema de governança de tecnologia da informação e comunicação, sob a coordenação do Comitê de Governança de Tecnologia da Informação e Comunicação;

XIV - promover, coordenar e acompanhar as ações relacionadas à segurança cibernética e da informação;

XV - manter interlocução com os demais comitês e unidades administrativas da JMU, a fim de conciliar a execução das ações de segurança cibernética e da informação;

XVI - encaminhar demandas e projetos ao Comitê de Governança de Tecnologia da Informação e Comunicação para deliberação quanto à priorização, conveniência e capacidade de execução;

XVII - acompanhar regulamentações no âmbito do Poder Judiciário e monitorar o cumprimento de determinações provenientes da Autoridade Nacional de Proteção de Dados (ANPD) com relação ao tratamento e proteção de dados pessoais;

XVIII - elaborar o protocolo de prevenção a incidentes cibernéticos;

XIX - elaborar o plano de ação do protocolo de gerenciamento de crise cibernética;

XX - definir mecanismos de respostas e prevenção, contemplando funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas;

XXI - propor ações que visem ao registro de informações relevantes para a investigação de ilícitos cibernéticos;

XXII - propor o Plano de Dados Abertos e definir o modelo formal para orientar as ações de implementação e promoção de abertura de dados;

XXIII - propor o Plano de Tratamento de Risco com base na Declaração de Aplicabilidade para implementar a segurança da informação e privacidade;

XXIV - rever a Política a cada 2 (dois) anos e monitorar as normas editadas sobre os temas abordados nesta Política;

XXV - propor critérios de classificação das informações administrativas, a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade, dados sensíveis e necessidade de compartilhamento.

Art. 42. O Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos se reunirá, ordinariamente, uma vez a cada seis meses, e adotará as seguintes regras para deliberação e convocação:

I - a reunião só será iniciada com a presença de, no mínimo, 2/3 (dois terços) dos membros;

II - as deliberações serão registradas em Ata pelo Secretário que será escolhido conforme a matéria a ser tratada;

III - as deliberações do Comitê serão tomadas pela maioria dos votos entre os membros presentes;

IV - os membros poderão solicitar convocações extraordinárias desde que autorizadas pelos coordenadores do Comitê.

Art. 43. As unidades gestoras da segurança cibernética e da informação proporão ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos, no prazo máximo de 180 (cento e oitenta) dias, contados a partir da publicação desta Resolução, seus respectivos planos decorrentes da presente Política.

Art. 44. As propostas de treinamento e capacitação poderão ser apresentadas por qualquer unidade administrativa da JMU e serão dirigidas ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA).

Parágrafo único. O Comitê fará uma análise preliminar acerca da conveniência da proposta e, caso entenda oportuna, encaminhará a proposta à Diretoria de Pessoal, para as devidas providências.

Seção IX

Das Competências e Responsabilidades

Art. 45. Compete aos Magistrados, Servidores, Colaboradores da JMU e Usuários de TIC:

I - adotar critérios de classificação e procedimentos de acesso às informações, observados os dispositivos legais e normas internas referentes ao sigilo e a outros requisitos de classificação;

II - zelar pela segurança cibernética sob sua custódia, conforme os critérios definidos em normativos;

III - comunicar, tempestivamente, ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos situações que comprometam a segurança cibernética sob sua custódia, ou aqueles casos em que não haja absoluta segurança quanto à proteção de documentos, dados, equipamentos, arquivos ou outros procedimentos necessários ao trato da informação;

IV - cumprir e fazer cumprir as normas estabelecidas na Política e nas demais diretivas relacionadas ao emprego dos sistemas e equipamentos de informática;

V - comunicar ao Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos eventuais limitações ao cumprimento dos critérios definidos para segurança cibernética;

VI - incorporar, nos processos de trabalho, práticas inerentes à segurança cibernética e da informação;

VII - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de violação à Política de Segurança da Informação;

VIII - implementar controles e monitoramentos de segurança pertinentes, sob a orientação técnica do Comitê Executivo.

Art. 46. Compete à Diretoria-Geral (DIREG):

I - instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

II - definir a missão, público-alvo, modelo de implementação, nível de autonomia, designação de integrantes, canal de comunicação de incidentes de segurança e os serviços que serão prestados;

III - normatizar a amplitude de autonomia técnica para atuação do grupo operacional técnico da Diretoria de Tecnologia da Informação e da ETIR, no caso de detecção de incidentes;

IV - apresentar ao Comitê de Governança de Tecnologia da Informação e Comunicação os estudos, normas e planos de ação propostos pelos Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos, Comitê de Gestão de Tecnologia da Informação e Comunicação e Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética.

Art. 47. Compete à Corregedoria da Justiça Militar:

I - auxiliar na elaboração do relatório de impacto à proteção de dados pessoais, solicitada pela autoridade nacional, no tocante à preservação de informações pessoais, em atividades de investigação e repressão de infrações penais;

II - adotar e monitorar em atividades de correição geral ou especial, medidas eficazes e capazes de comprovar o cumprimento das normas de privacidade, segurança da informação e cibernética e dados abertos;

III - definir forma de atuação negocial diante de incidentes de segurança de dados e informação na primeira instância.

Art. 48. Compete à Diretoria de Documentação e Gestão do Conhecimento (DIDOC):

I - propor normas e procedimentos para proteção, reprodução, digitalização, manuseio, remoção, exposição, empréstimo, trânsito, guarda, conservação e restauração do acervo documental, museológico e bibliográfico da JMU em suporte físico ou digital;

II - designar o responsável por cada acervo de que trata o inciso I para acompanhar o acervo em trânsito, dentro e fora da JMU;

III - propor investimentos relacionados à segurança da tecnologia da informação, com a finalidade de minimizar e eliminar vulnerabilidades e comprometimentos das informações custodiadas na JMU;

IV - avaliar os incidentes de segurança, a disponibilização dos dados abertos e privacidade e propor ações corretivas para assegurar a eficácia e a contínua pertinência desta Política;

V - coordenar e cumprir a metodologia estabelecida pela legislação vigente para a eliminação de documentos arquivísticos físicos, digitais e eletrônicos;

VI - realizar, em compartilhamento com a Diretoria de Tecnologia da Informação, os procedimentos técnicos de eliminação de documentos arquivísticos digitais e eletrônicos;

VII - definir, com a Diretoria de Tecnologia da Informação, os *hardwares* e *softwares* que comporão o RDC-Arq, bem como os sistemas informacionais correlatos à área de segurança da informação referente aos documentos arquivísticos;

VIII - elaborar, executar e acompanhar o Plano de Preservação de Documentos Digitais - PPDD, dados, processos e documentos digitais e digitalizados, em coparticipação da Diretoria de Tecnologia da Informação;

IX - coordenar, executar e acompanhar a segurança da informação, de documentos, de processos e dos materiais bibliográficos em suporte físico.

Art. 49. Compete à Diretoria de Tecnologia da Informação (DITIN) e à Coordenadoria de Tecnologia (COTEC):

I - propor e executar medidas necessárias a fim de restringir os poderes de cada usuário de TIC dos sistemas, com vistas a impedir que pessoas possam excluir os registros e trilhas de auditoria das suas próprias ações;

II - garantir segurança especial para sistemas com acesso público;

III - planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida no Processo Judicial Eletrônico (e-Proc/JMU), Sistema Eletrônico de Informações - SEI-JMU e demais sistemas judiciais e administrativos da JMU;

IV - planejar e executar as atividades visando à manutenção das cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a JMU;

V - planejar a implantação de comandos em sistemas de modo a gerar registros auditáveis de informações e dados regidos pelos princípios de confidencialidade, integridade, acessibilidade, disponibilidade e autenticidade;

VI - definir normas e padrões para monitoramento do ambiente de TIC, gerando indicadores e históricos de:

a) tempo de resposta no acesso e períodos de indisponibilidade da internet e de sistemas críticos;

b) incidentes de segurança, tais como vírus, *trojans*, furtos, acessos indevidos e outras ameaças;

c) uso da capacidade instalada da rede e dos equipamentos;

d) acesso à internet e aos sistemas críticos e atividade de todos os usuários de TIC durante os acessos às redes externas;

VII - planejar e executar as atividades de segurança, bem como estabelecer normas para uso da internet, intranet e correio eletrônico de forma a esclarecer os usuários de TIC sobre atividades permitidas e proibidas;

VIII - realizar, em compartilhamento com a Diretoria de Documentação e Gestão do Conhecimento, os procedimentos técnicos de eliminação de documentos arquivísticos digitais e eletrônicos;

IX - executar o protocolo de prevenção a incidentes cibernéticos;

X - instituir processo formalmente definido, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Art. 50. Compete a Coordenadoria de Apoio Jurisdicional (COAJU):

I - propor estudos relacionados à segurança da tecnologia da informação, com objetivo de reduzir ou eliminar as fragilidades dos sistemas judiciais da JMU, a fim de evitar comprometimento, perda e corrupção das informações;

II - avaliar possíveis incidentes de segurança na disponibilização dos serviços de consulta processual e consulta de jurisprudência e propor ações corretivas assegurando a efetividade desta Política;

III - realizar, em compartilhamento com a Diretoria de Tecnologia da Informação e a Diretoria de Documentação e Gestão do Conhecimento a execução e o acompanhamento do Plano de Preservação de Documentos Digitais - PPDD referentes aos dados constantes no sistema de Processo Judicial Eletrônico (e-Proc/JMU).

Art. 51. Compete ao Comitê Executivo do SEI-JMU:

I - propor normas e implementar procedimentos para bloquear usuários inativos do SEI-JMU no controle de acesso ao sistema;

II - definir procedimento de autorização formal para a concessão e a revogação de acesso ao sistema administrativo da JMU;

III - avaliar as ocorrências de falhas na segurança cibernética e da informação, bem como dos dados que requerem privacidade e recomendar ações corretivas;

IV - fazer projeções de necessidades de capacidade futura, para evitar potenciais gargalos e garantir o desempenho do Sistema Eletrônico de Informações;

V - definir procedimentos padronizados para monitorar as atividades dos usuários de TIC no sistema administrativo em coparticipação com a Diretoria de Tecnologia da Informação.

Seção X

Do Monitoramento e Da Auditoria Do Ambiente

Art. 52. Para garantir o cumprimento da Política de Privacidade, Segurança Cibernética e Gestão de Dados fica autorizado:

I - implantação de sistemas de monitoramento em estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou outros componentes da rede, resguardados o direito à privacidade e o sigilo da correspondência, na forma da lei;

II - utilização dos relatórios gerados pelos diversos sistemas de informação para identificar os usuários, os respectivos acessos efetuados e o material manipulado;

III - realização, a qualquer tempo, a inspeção física nas máquinas, aparelhos e demais equipamentos, fixos e móveis, de propriedade da Justiça Militar da União;

IV - instalação de sistemas de proteção, preventivos e detectáveis, para garantir a segurança cibernética e da informação e dos perímetros de acesso;

V - possibilidade de tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou processo administrativo;

VI - aos usuários que desejarem usar os serviços de rede da Justiça Militar da União com recursos tecnológicos não disponibilizados pela Diretoria de Tecnologia da Informação deverão assinar o Termo de Concordância e Adesão, anexo II, desta Política.

Seção XI

Da Classificação, Do Sigilo Da Informação, Da Garantia e Do Controle De Acesso

Art. 53. A publicidade de informações é preceito geral, e o sigilo é exceção, conforme art. 3º, inciso I, Resolução nº 240/2017.

§ 1º Qualquer falha na segurança da informação, relacionada à garantia ou ao controle de acesso, identificada por qualquer usuário, deve ser imediatamente comunicada ao seu superior imediato, que a encaminhará à Diretoria de Tecnologia da Informação para avaliação e determinação de ações corretivas.

§ 2º O acesso a sistemas de informação da JMU deve ser controlado de acordo com o valor, sensibilidade e criticidade da informação nele contida e considerando aspectos de restrição legais ou normativos.

Art. 54. A classificação da informação tem por objetivo assegurar um nível adequado de proteção.

§ 1º A informação deve ser classificada por quem a gerou, para indicar a necessidade, as prioridades e o nível esperado de proteção durante todo o seu ciclo de vida.

§ 2º Toda informação não classificada terá caráter ostensivo e deverá ser fornecida a qualquer cidadão identificado que a solicitar, em formato aberto, independentemente de motivação, exceto a coberta por segredo de justiça ou outro caráter de sigilo.

Art. 55. As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual da JMU e não cabe a seus criadores qualquer forma de restrição de acesso.

Parágrafo único. Quando as informações forem produzidas por colaboradores para uso exclusivo pela JMU, instrumento próprio estabelecerá as obrigações dos criadores, inclusive no que se refere à eventual confidencialidade.

Art. 56. O processo de controle de acesso à informação tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança cibernética e da informação.

§ 1º O acesso às informações não públicas produzidas ou custodiadas deve permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso a informações não públicas por quaisquer colaboradores é condicionado ao aceite de termo de sigilo e responsabilidade.

§ 3º O acesso às informações produzidas ou custodiadas pela JMU submete quem a acessa a controles administrativos e tecnológicos definidos de acordo com a respectiva classificação.

Art. 57. Todos os usuários que manipulem ou tenham acesso a informações identificadas como sigilosas, sob custódia ou de propriedade da JMU, devem garantir a confidencialidade e o segredo dessas informações.

Parágrafo único. Sem autorização, é vedada qualquer forma de impressão, transmissão, compartilhamento ou transporte de informação sigilosa para fora das instalações da JMU.

Art. 58. A inobservância dos dispositivos desta Resolução pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 59. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela JMU devem observar, no que couber, as disposições desta Resolução.

CAPÍTULO IV

Seção I

Dos Dados Abertos

Art. 60. Os dados abertos da Justiça Militar da União atendem a premissas do interesse público, publicidade, transparência, eficiência e eficácia.

§ 1º O atendimento aos princípios é baseado nos seguintes critérios:

I - grau de relevância ao cidadão;

II - dados mais solicitados em transparência passiva;

III - estímulo ao controle e à participação social;

IV - promoção ao combate à corrupção;

V - obrigatoriedade legal de disponibilização de dados;

VI - resultados diretos e efetivos dos serviços públicos;

VII - possibilidade de fomento a novos negócios na sociedade;

VIII - alinhamento ao Planejamento Estratégico do JMU.

Art. 61. O Portal de Dados Abertos da JMU deve garantir os seguintes requisitos técnicos:

I **-** Controle de acesso: somente as pessoas autorizadas devem ter acesso para publicação e modificação dos dados e metadados;

II **-** Integridade: assegurar que os dados não sejam adulterados durante a transferência;

III **-** Autenticidade: assegurar que os dados provêm de uma fonte legítima da Justiça Militar da União.

Art. 62. No processo de monitoramento e controle das ações de implantação dos dados abertos serão observados os indicadores e as principais demandas encaminhadas a JMU, provenientes de reclamações recebidas pela Ouvidoria da Justiça Militar da União.

Art. 63. Não será permitido nenhum instrumento jurídico que impeça a reutilização e redistribuição por qualquer parte da sociedade dos dados aberto da Justiça Militar da União.

Art. 64. Serão disponibilizadas bases de dados em estado bruto, para serem livremente manipuladas, filtradas ou cruzadas com outras, inclusive permitindo a construção de novas aplicações e conhecimentos.

Art. 65. A matriz de priorização e limites dos dados abertos será regulamentada em norma própria.

CAPÍTULO V

Seção I

Das Disposições Finais

Art. 66. Os casos omissos serão resolvidos pelo Controlador e Controlador Adjunto dos Dados ouvido o Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos.

ANEXO II

TERMO DE CONCORDÂNCIA E ADESÃO

Pelo presente termo, declaro ter conhecimento da Política de Privacidade, Segurança Cibernética e Dados Abertos da Justiça Militar da União - JMU, disponível para consulta no sítio da internet http://www.stm.jus.br e concordo em aceitar as regras.

Com autorização superior, estou recebendo uma conta com privilégios adequados ao exercício das atividades, que aqui executo, a qual deverá ser utilizada somente para tal fim.

Em face dos recursos computacionais[i] recebidos declaro estar ciente e comprometido:

1. com o uso pessoal e intransferível da credencial eletrônica[ii] para acesso ao ambiente tecnológico corporativo da JMU.

2. com o uso do ambiente tecnológico corporativo da instituição, exclusivamente para exercício de minhas atribuições e o desempenho de minhas atividades funcionais.

3. com a confidencialidade e salvaguarda das informações por mim acessadas que trafegam no ambiente tecnológico corporativo da JMU, em decorrência de credencial eletrônica e/ou outro meio de acesso.

4. com a responsabilidade de transmitir aos demais colaboradores da minha unidade organizacional (terceirizados, contratados, entre outros agentes externos), o teor do presente termo de responsabilidade e a compulsoriedade do seu cumprimento.

Declaro estar ciente de que minhas ações serão monitoradas de acordo com a Política de Privacidade, Segurança Cibernética e Dados Abertos da JMU e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

Estou ciente, ainda, de minha responsabilidade pelo dano que possa causar por descumprimento da Política de Privacidade, Segurança Cibernética e Dados Abertos da JMU ao realizar uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura. E por estar de acordo com o inteiro teor deste Termo, assino nesta data, para que produza seus jurídicos e legais efeitos.

---

[i] São exemplos dos componentes que fazem parte dos recursos computacionais: rede de computadores, ativos de rede que permitem o funcionamento desta rede e seu acesso a outras redes (como é o caso da internet), equipamentos de segurança da informação e Sistemas de Informação.

[ii] É a identidade digital requerida para acessar o ambiente tecnológico corporativo da JMU. É composto pelo binômio das informações de: (1) identificação do usuário (login) e (2) sua respectiva senha. Esta credencial é fornecida pela DITIN a cada colaborador da instituição que precise acessar o ambiente tecnológico corporativo sob sua gestão.

Documento assinado eletronicamente por **LUIS CARLOS GOMES MATTOS**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 06/08/2021, às 16:23 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2277398** e o código CRC **216EEC81**.

2277398v5